

# Guia de implantação de redundância de HA CSR1000v no Amazon AWS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Meta](#)

[Topologia](#)

[Diagrama de Rede](#)

[Terminology](#)

[Restrições](#)

[Configuração](#)

[Etapa 1. Escolha uma Região.](#)

[Etapa 2. Criar um VPC.](#)

[Etapa 3. Criar um Grupo de Segurança para o VPC.](#)

[Etapa 4. Criar uma função IAM com uma Política e associá-la ao VPC.](#)

[Etapa 5. Inicie o CSR1000v com a função AMI que você criou e associe as sub-redes públicas/privadas.](#)

[Etapa 6. Repita a Etapa 5 e crie a segunda instância do CSR1000v para HA.](#)

[Etapa 7. Repita a Etapa 5 e crie uma VM \(Linux/Windows\) no AMI Marketplace.](#)

[Etapa 8. Configurar as tabelas de rotas privadas e públicas.](#)

[Etapa 9. Configurar a conversão de endereço de rede \(NAT\) e o túnel GRE com BFD e qualquer protocolo de roteamento.](#)

[Etapa 10. Configurar a alta disponibilidade \(Cisco IOS XE Denali 16.3.1a ou posterior\).](#)

[Verifique a alta disponibilidade](#)

[Troubleshoot](#)

[Problema: falha na `httpc\_send\_request`](#)

[Problema: a tabela de rota `rtb-9c000f4` e a interface `eni-32791318` pertencem a redes diferentes](#)

[Problema: Você não está autorizado a executar esta operação. Mensagem de falha de autorização codificada.](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve o guia de configuração sobre como implantar roteadores CSR1000v para alta disponibilidade na nuvem do Amazon AWS. O objetivo é fornecer aos usuários conhecimento prático de HA e a capacidade de implantar um ambiente de teste totalmente funcional.

Para obter informações mais detalhadas sobre AWS e HA, *consulte* a seção.

# Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Uma conta Amazon AWS
- 2 CSR1000v e 1 AMIs Linux/Windows na mesma região
- O HA versão 1 é suportado no Cisco IOS-XE® versões 16.5 a 16.9. A partir de 16.11, use a versão 3 do HA.

## Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS-XE® Denali 16.7.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Meta

Em um ambiente com várias zonas de disponibilidade, simule o tráfego contínuo do data center privado (VM) para a Internet. Simule um failover de HA e observe que o HA é bem-sucedido quando a tabela de roteamento comuta o tráfego de CSRHA para a interface privada de CSRHA1 é confirmada.

## Topologia

Antes de iniciar a configuração, é importante entender a topologia e o projeto completamente. Isso ajuda a solucionar qualquer problema potencial posteriormente.

Há vários cenários de implantação de HA com base nos requisitos de rede. Para este exemplo, a redundância de HA é configurada com estas configurações:

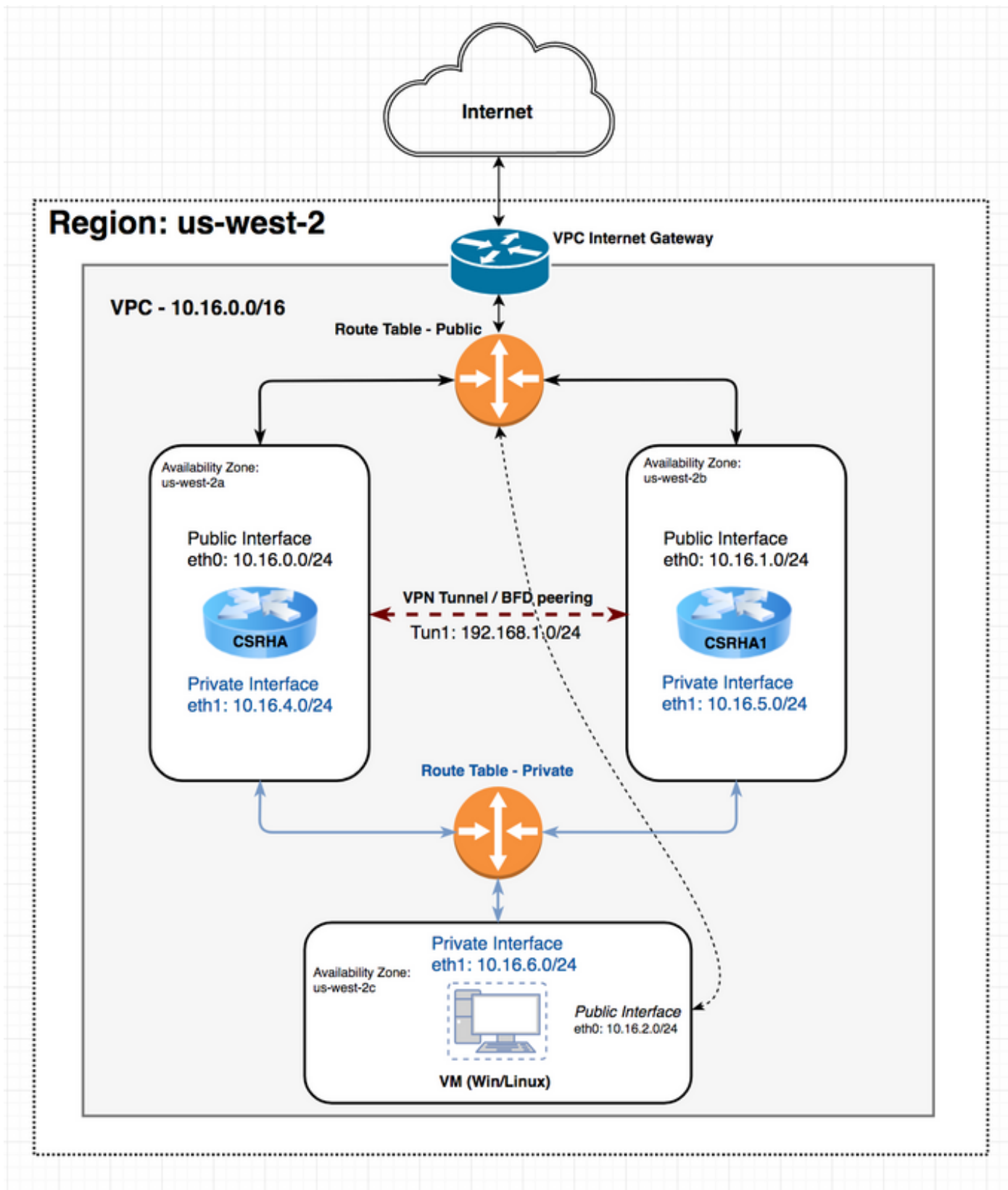
- 1x - Região
- 1x - VPC
- 3x - Zonas de disponibilidade
- 6x - Interfaces/sub-redes de rede (3x pública/3x privada)
- 2x - Tabelas de rota (pública e privada)
- 2x - Roteadores CSR1000v (Cisco IOS-XE® Denali 16.3.1a ou posterior)
- 1x - VM (Linux/Windows)

Há 2x roteadores CSR1000v em um par HA, em duas zonas de disponibilidade diferentes. Pense em cada zona de disponibilidade como um data center separado para obter resiliência de hardware adicional.

A terceira zona é uma VM, que simula um dispositivo em um data center privado. Por enquanto, o acesso à Internet é habilitado através da interface pública no para que você possa acessar e configurar a VM. Geralmente, todo o tráfego normal deve fluir pela tabela de rotas privadas.

Faça ping na interface privada da VM → tabela de rota privada → CSRHA → 8.8.8.8 para simulação de tráfego. Em um cenário de failover, observe que a tabela de rota privada alternou a rota para apontar para a interface privada do CSRHA1.

## Diagrama de Rede



## Terminology

RTB - A ID da tabela de rotas.

CIDR - Endereço de destino para a rota a ser atualizada na tabela de rotas.

ENI - O ID da interface de rede da interface gigabit CSR 1000v para a qual o tráfego é roteado. Por exemplo, se o CSRHA falhar, o CSRHA1 assumirá e atualizará a rota na tabela de rotas AWS para apontar para seu próprio ENI.

REGIÃO - A região AWS do CSR 1000v.

## Restrições

- Para sub-redes privadas, não use o endereço IP 10.0.3.0/24 — ele é usado internamente no Cisco CSR 1000v para alta disponibilidade. O Cisco CSR 1000v precisa ter acessibilidade pública à Internet para fazer chamadas à API REST que alteram a tabela de rotas AWS.
- Não coloque a interface gig1 do CSR1000v dentro de um VRF. O HA não funciona de outra forma.

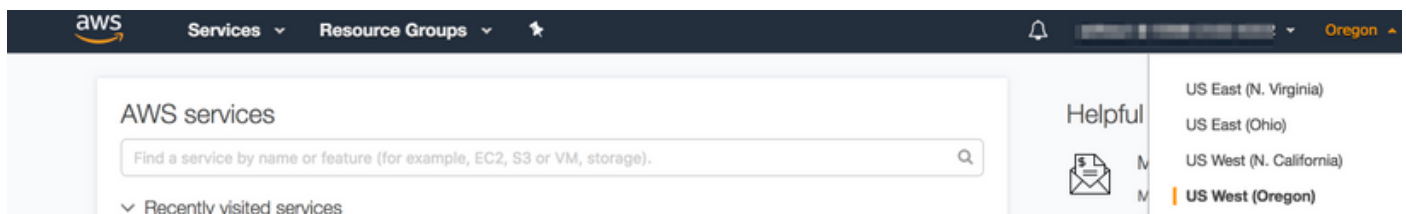
## Configuração

O fluxo geral de configuração é começar no recurso mais abrangente superior (Região/VPC) e descer até o mais específico (Interface/sub-rede). No entanto, não há uma ordem específica de configuração. Antes de começar, é importante entender a topologia primeiro .

**Tip:** Dê nomes a todas as suas configurações (VPC, Interface, Sub-rede, Tabelas de Rotas, etc.).

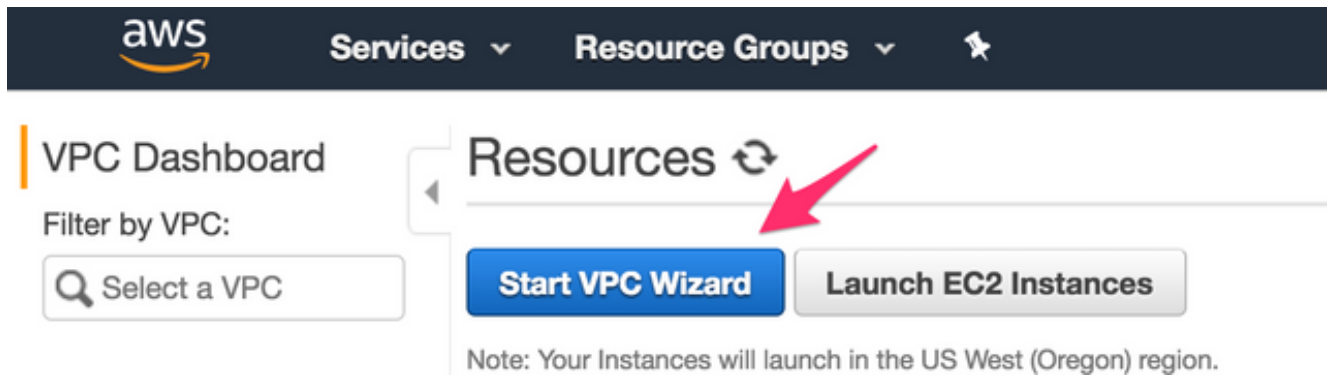
### Etapa 1. Escolha uma Região.

Este exemplo usa US West (Oregon).



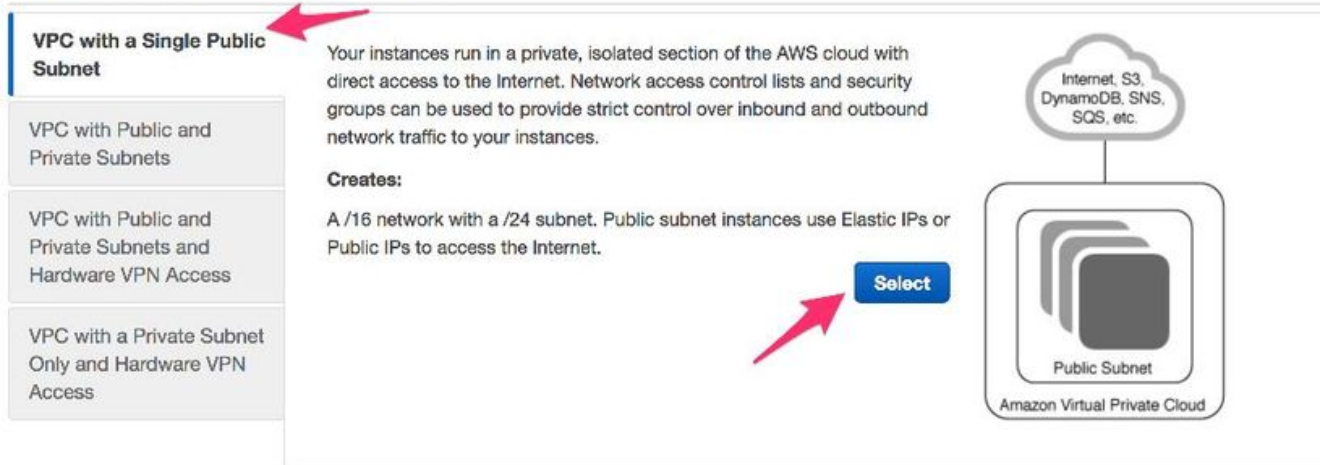
### Etapa 2. Criar um VPC.

1. No AWS Console, navegue para **VPC > VPC Dashboard > Start VPC Wizard**.



## 2. Escolha VPC com uma única sub-rede pública.

Step 1: Select a VPC Configuration

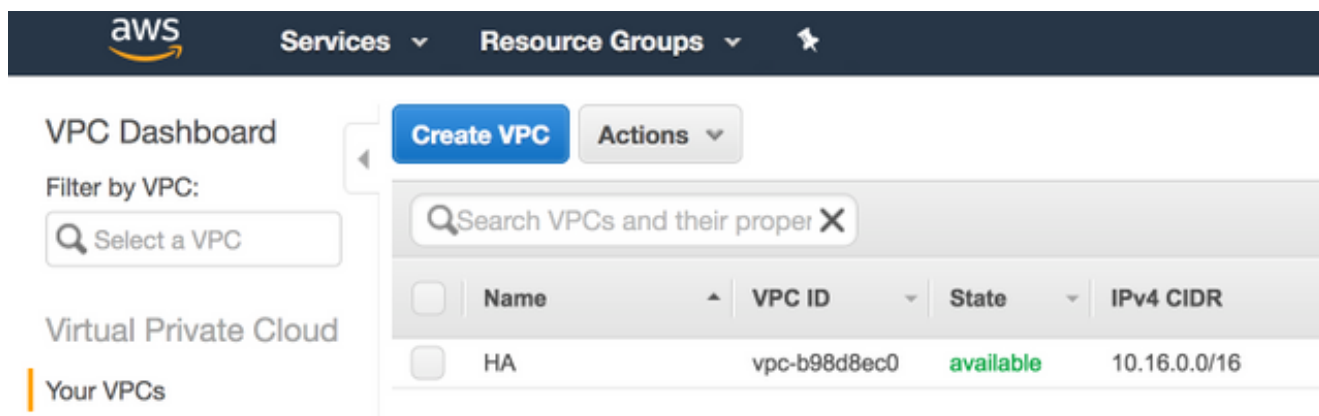


## 3. Ao criar um VPC, você recebe uma rede /16 para usar como desejar.

## 4. Você também recebe uma sub-rede pública /24. As instâncias de sub-rede públicas usam IPs elásticos ou IPs públicos para que seus dispositivos acessem a Internet.



## 5. vpc-b98d8ec0 é criado.



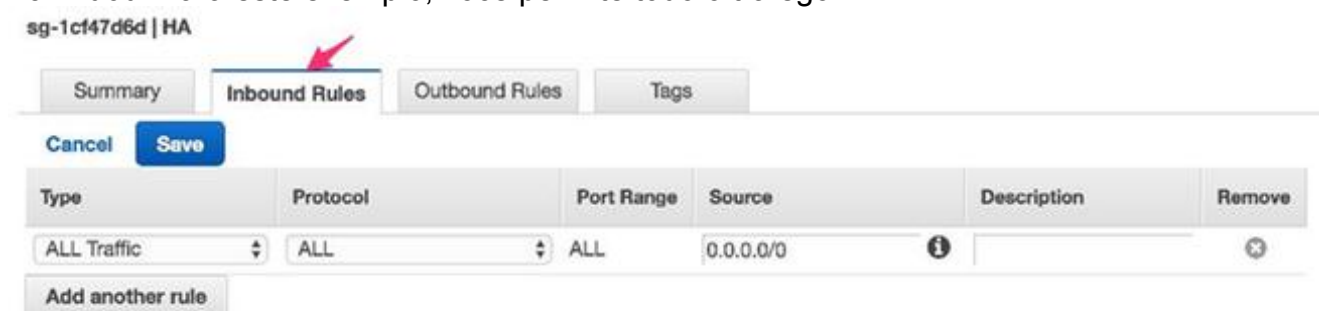
### Etapa 3. Criar um Grupo de Segurança para o VPC.

Os grupos de segurança são como ACLs para permitir ou negar tráfego.

1. Em Segurança, clique em **Grupos de segurança** e **Crie seu grupo de segurança** associados ao VPC criado acima chamado HA.



2. Em Inbound Rules (Regras de entrada), defina que tráfego você deseja permitir para sg-1cf47d6d. Para este exemplo, você permite todo o tráfego.

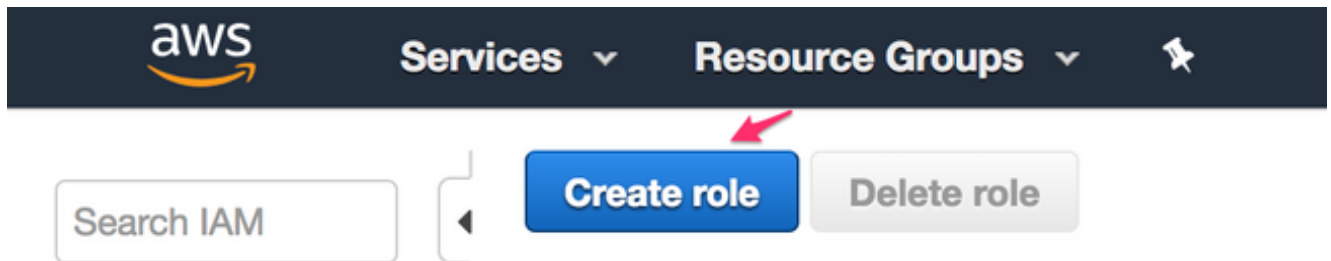


### Etapa 4. Criar uma função IAM com uma Política e associá-la ao VPC.

O IAM concede ao seu CSR acesso às APIs da Amazon.

O CSR1000v é usado como um proxy para chamar comandos API do AWS para modificar a tabela de rotas. Por padrão, as AMIs não têm permissão para acessar as APIs. Este procedimento cria uma função IAM e essa função é usada durante o início de uma instância CSR. O IAM fornece as credenciais de acesso para que os CSRs usem e modifiquem as APIs do AWS.

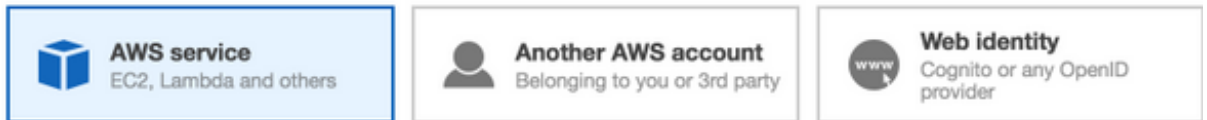
1. Criar função IAM. Navegue até o painel IAM e vá até **Funções > Criar função**, conforme mostrado na imagem.



2. Como mostrado na imagem, permita que a instância EC2 chame o AWS em seu nome.

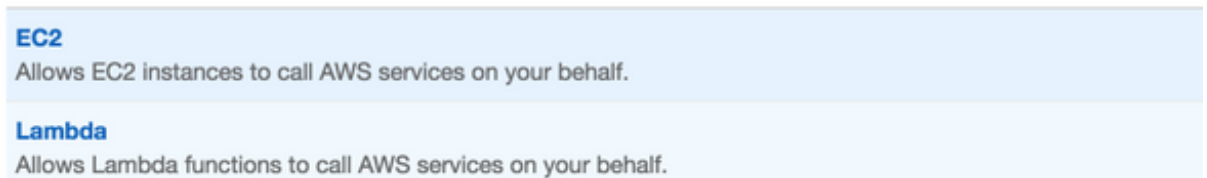
## Create role

### Select type of trusted entity



Allows AWS services to perform actions on your behalf. [Learn more](#)

### Choose the service that will use this role



3. Crie uma função e clique em **Avançar: Revisar**, conforme mostrado na imagem.

## Create role

1 2 3

### Attach permissions policies

Choose one or more policies to attach to your new role.

[Create policy](#) [Refresh](#)

Filter: Policy type  Showing 394 results

<input type="checkbox"/>	Policy name	Attachments	Description
<input type="checkbox"/>	AdministratorAccess	7	Provides full access to AWS services and resources.
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	0	Provide device setup access to AlexaForBusiness services
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	Grants full access to AlexaForBusiness resources and acces...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	Provide gateway execution access to AlexaForBusiness serv...
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	0	Provide read only access to AlexaForBusiness services
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	Provides full access to create/edit/delete APIs in Amazon AP...
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	Provides full access to invoke APIs in Amazon API Gateway.
<input type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	0	Allows API Gateway to push logs to user's account.
<input type="checkbox"/>	AmazonAppStreamFullAccess	0	Provides full access to Amazon AppStream via the AWS Ma...
<input type="checkbox"/>	AmazonAppStreamReadOnlyAccess	0	Provides read only access to Amazon AppStream via the AW...
<input type="checkbox"/>	AmazonAppStreamServiceAccess	0	Default policy for Amazon AppStream service role.
<input type="checkbox"/>	AmazonAthenaFullAccess	0	Provide full access to Amazon Athena and scoped access to...

\* Required

[Cancel](#) [Previous](#) [Next: Review](#)

4. Dê um nome de função a ele. Para este exemplo, como mostrado na imagem, o nome da função é **routetablechange**.

# Create role

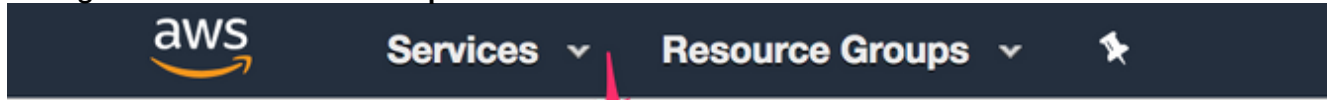
## Review

Provide the required information below and review this role before you create it.

Role name\*

Use alphanumeric and '+,=,@-\_' characters. Maximum 64 characters.

5. Em seguida, você precisa criar uma política e anexá-la à função criada acima. Painele IAM e navegue até Políticas > Criar política.



Search IAM

Create policy

Policy actions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateRouteTable",
        "ec2>DeleteRoute",
        "ec2>DeleteRouteTable",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:ReplaceRoute",
        "ec2:DisassociateRouteTable",
        "ec2:ReplaceRouteTableAssociation"
      ],
      "Resource": "*"
    }
  ]
}
```

## Create policy

1

2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

This policy validation failed and might have errors converting to JSON: The policy must have at least one statement For more information about the IAM policy grammar, see [AWS IAM Policies](#)

Visual editor

JSON

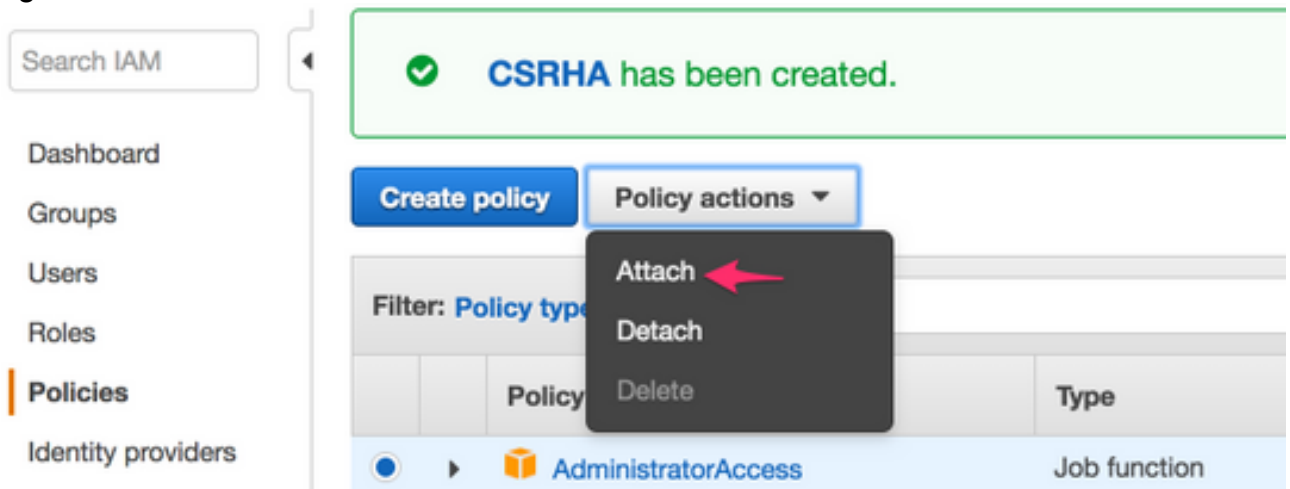
[Import managed policy](#)

```
1- [
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "ec2:AssociateRouteTable",
8-         "ec2:CreateRoute",
9-         "ec2:CreateRouteTable",
10-        "ec2>DeleteRoute",
11-        "ec2>DeleteRouteTable",
12-        "ec2:DescribeRouteTables",
13-        "ec2:DescribeVpcs",
14-        "ec2:ReplaceRoute",
15-        "ec2:DisassociateRouteTable".
```

6. Dê um nome de política a ele e anexe-o à Função que você criou. Para este exemplo, o



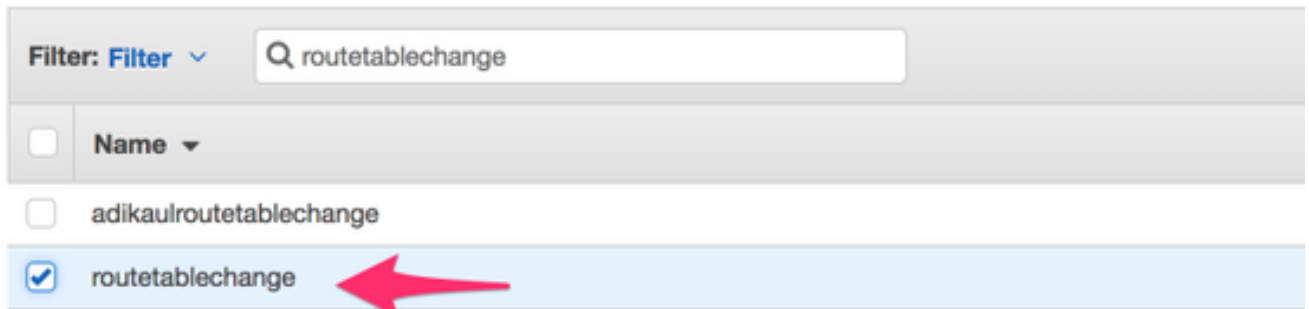
nome da política é chamado CSRHA com Acesso de Administrador, como mostrado na imagem.



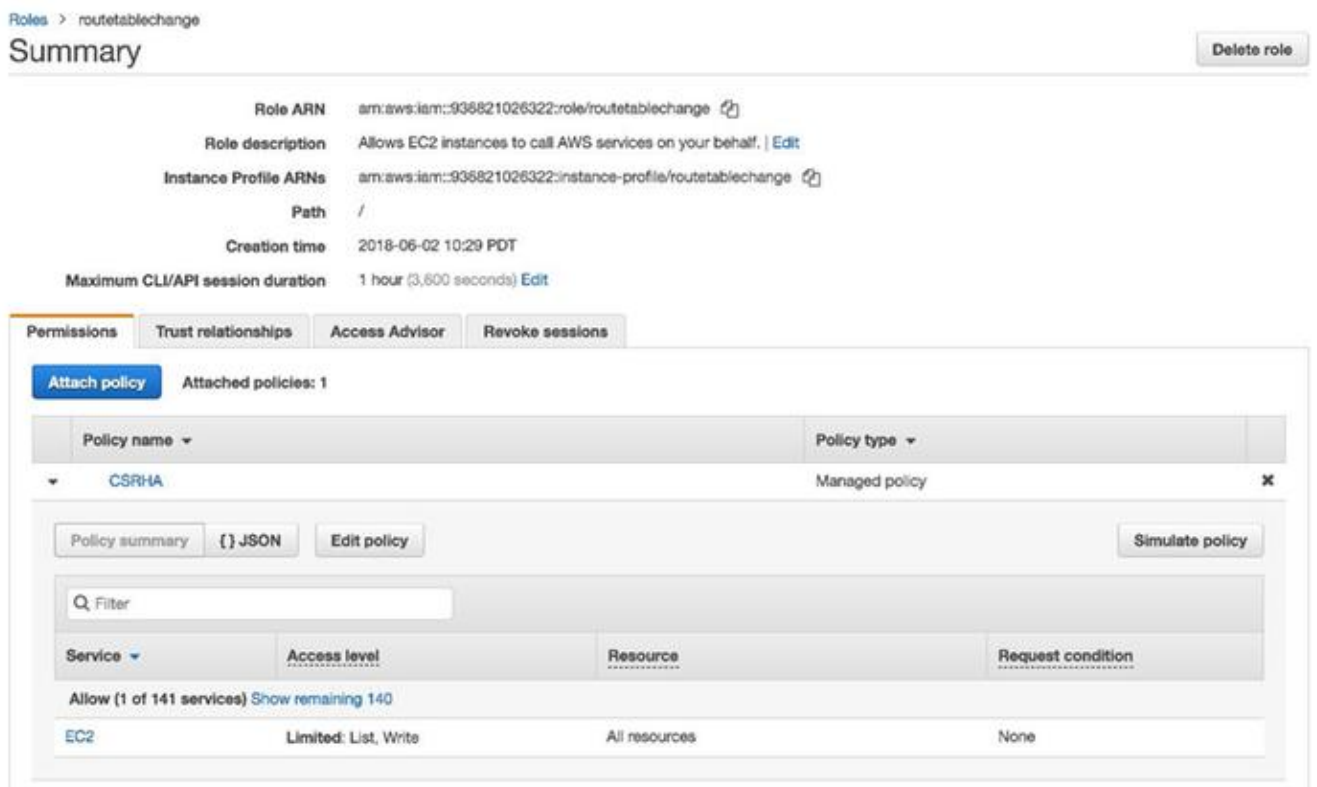
7. Como mostrado na imagem, anexe a política à função criada chamada **rutetablechange**.

### Attach Policy

Attach the policy to users, groups, or roles in your account.



8. Summary.



Etapa 5. Inicie o CSR1000v com a função AMI que você criou e associe as sub-

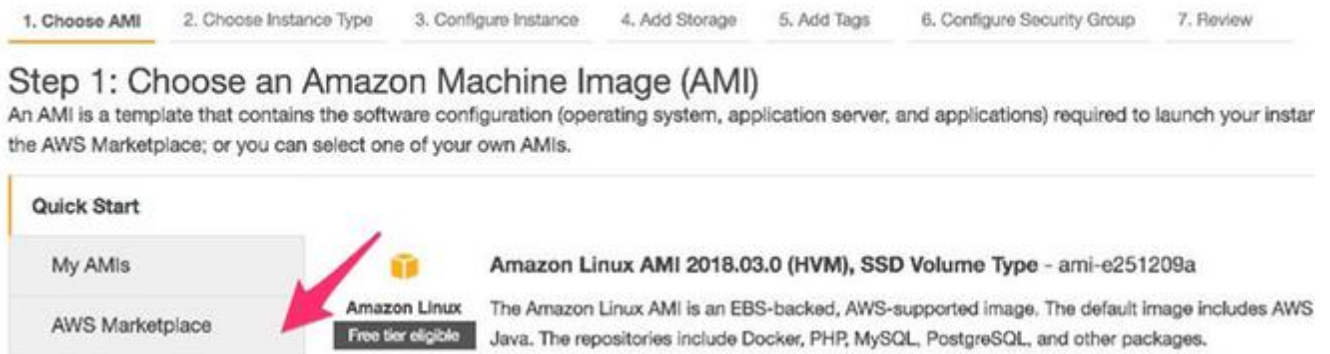
## redes públicas/privadas.

Cada roteador CSR1000v tem 2 interfaces (1 pública, 1 privada) e está em sua própria zona de disponibilidade. Você pode pensar em cada CSR como estando em data centers separados.

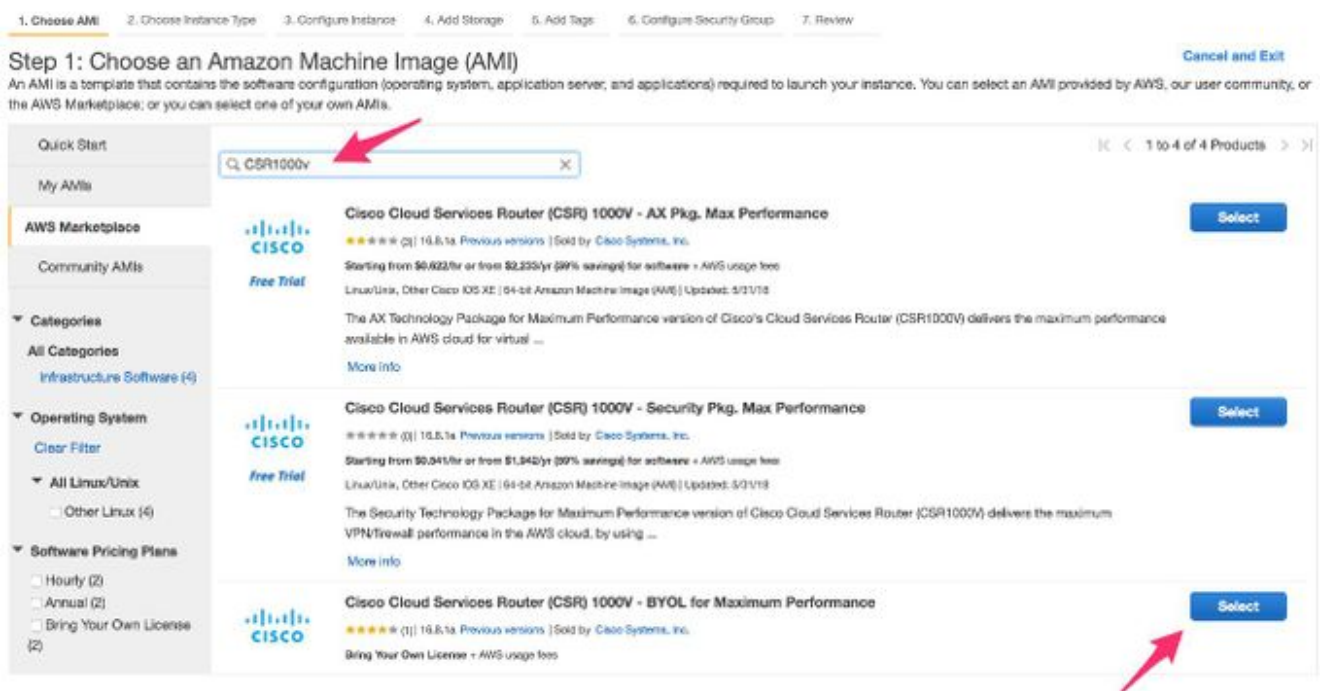
1. No console AWS, selecione **EC2** e clique em **Iniciar instância**.



2. Selecione AWS Marketplace.



3. Digite CSR1000v e, para este exemplo, use o Cisco Cloud Services Router (CSR) 1000V - BYOL para obter o máximo desempenho.



4. Escolha um Tipo de Instância. Para este exemplo, o tipo selecionado é **t2.medium**.

## Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell ES-2686v4, 4 GiB memory, EBS only)

Note: The vendor recommends using a c4.large instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes

5. Enquanto a Instância estiver configurada, você precisa certificar-se de selecionar o VPC criado acima junto com a função IAM acima. Além disso, crie uma sub-rede privada que você associa à interface privada.

## Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances  Launch into Auto Scaling Group

Purchasing option  Request Spot instances

Network    
No default VPC found. Create a new default VPC.

Subnet    
251 IP Addresses available

Auto-assign Public IP

Placement group  Add instance to placement group.

IAM role

Shutdown behavior

Enable termination protection  Protect against accidental termination

Monitoring  Enable CloudWatch detailed monitoring  
Additional charges apply.

6. Clique em Criar nova sub-rede para sub-rede privada. Para este exemplo, a marca Name é HA Private. Certifique-se de que esteja na mesma zona de disponibilidade que a sub-rede pública.

## Create Subnet



Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: HA Private

VPC: vpc-a6fefedf | HA

VPC CIDRs	CIDR	Status	Status Reason
	10.16.0.0/16	associated	

Availability Zone: us-west-2a

IPv4 CIDR block: 10.16.4.0/24

Cancel Yes, Create

7. Role para baixo e, em Configure Instance Details (Configurar detalhes da instância), clique em **Add Device**, conforme mostrado na imagem.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-66f7931f	Auto-assign	Add IP	

Add Device

8. Depois que a interface secundária for adicionada, associe a sub-rede privada que você criou chamada HA Private. Eth0 é a interface pública e Eth1 é a interface privada. **Note:** A sub-rede criada na etapa anterior pode não aparecer nesse menu suspenso. Talvez seja necessário atualizar ou cancelar a página e começar novamente para que a sub-rede seja exibida.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-66f7931f	Auto-assign	Add IP	
eth1	New network interface	subnet-66f7931f (Public subnet) 10.16.0.0/24 us-west-2a ✓ subnet-89c5a1f0 (HA Private) 10.16.4.0/24 us-west-2a			

9. Selecione o Grupo de segurança criado em VPC e verifique se as regras estão definidas corretamente.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group:  Create a new security group  Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-01880170	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-1cf47d6d	HA	HA	Copy to new

10. Crie um novo par de chaves e certifique-se de baixar sua chave privada. Você pode reutilizar uma chave para cada dispositivo. **Note:** Se você perder sua chave privada, não poderá fazer login no CSR novamente. Não há método para recuperar chaves.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

## Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

**Key pair name**

CSRHA

Download Key Pair

You have to download the **private key file** (\*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

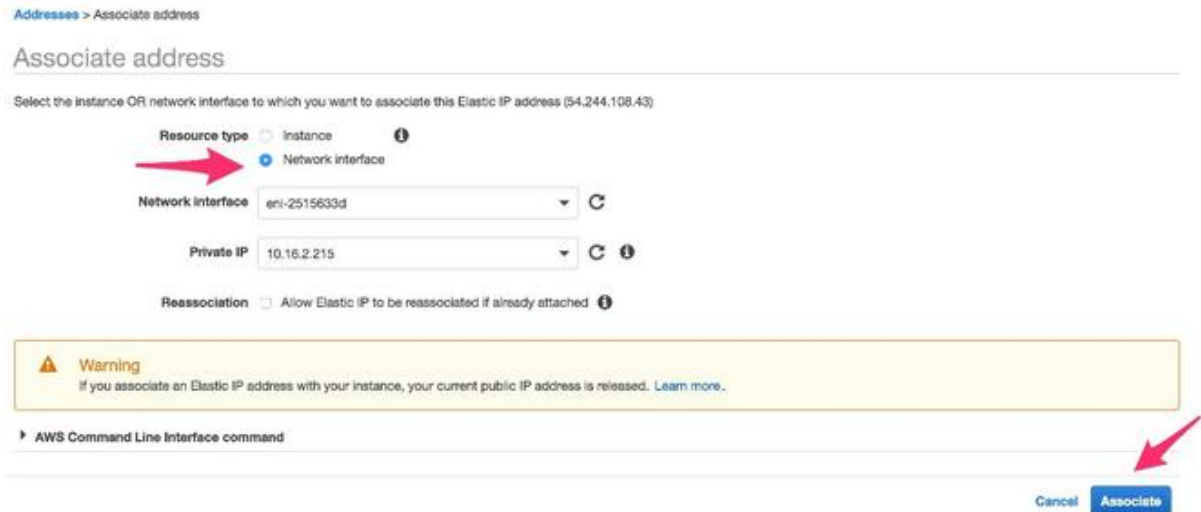
11. Associe o Elastic IP ao ENI da Interface Pública da instância criada e navegue até **Console AWS > EC2 Management > Network Security > Elastic IP's**. **Note:** A terminologia pública/privada pode confundir você aqui. Para os fins deste exemplo, a definição de uma interface pública é Eth0, que é a interface para a Internet. Do ponto de vista da AWS, nossa interface pública é seu ip privado.

EC2 Dashboard

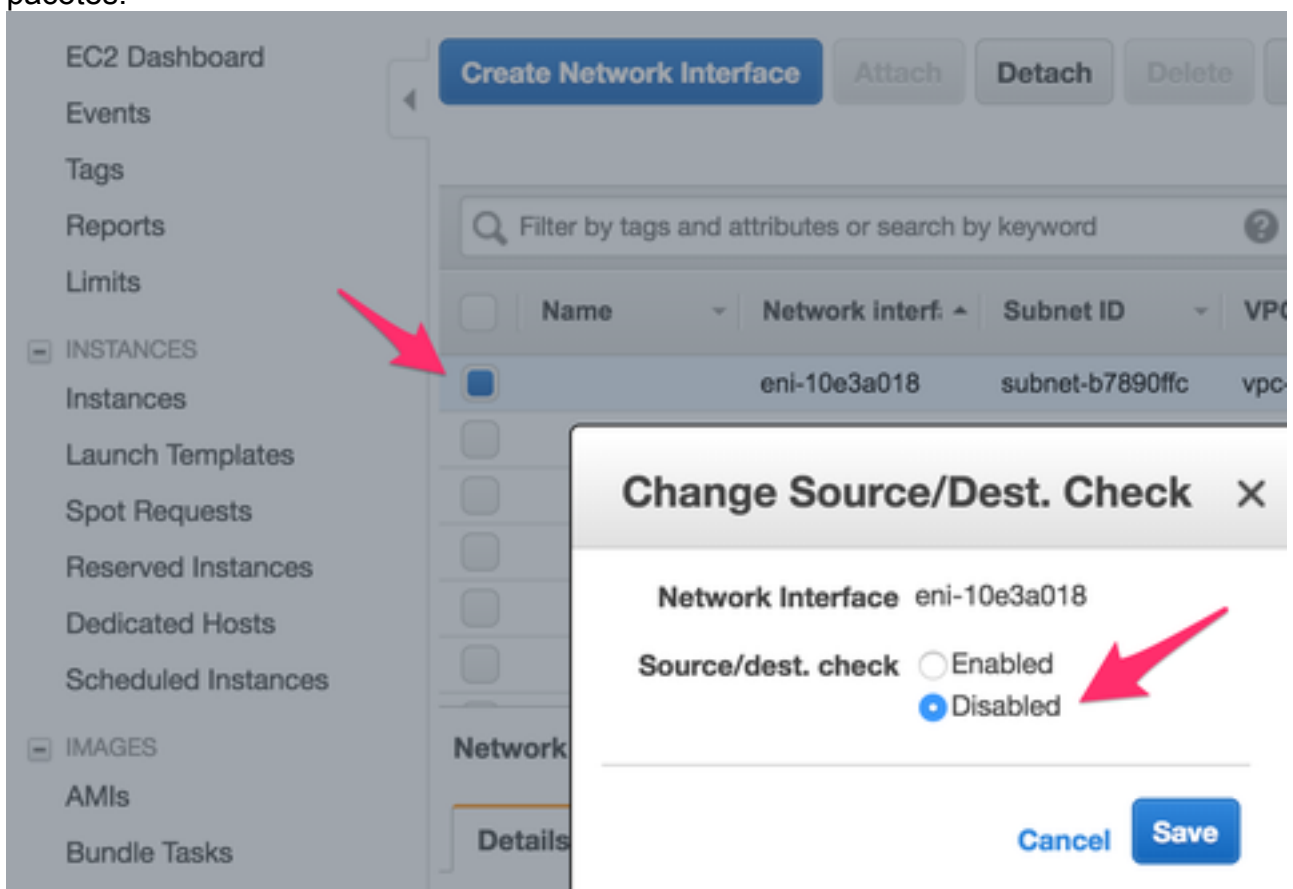
Events

Allocate new address

Actions



12. Desative a verificação de origem/destino enquanto navega para **EC2 > Interfaces de rede**. Verifique cada ENI para verificação de Origem/Destino. Por padrão, todos os ENIs vêm com essa verificação de origem/teste ativada. Um recurso anti-falsificação destinado a evitar que um ENI seja sobrecarregado com tráfego que não é realmente destinado a ele, verificando se o ENI é o destino do tráfego antes de encaminhá-lo. O roteador raramente é o destino real de um pacote. Este recurso deve ser desativado em todos os ENIs de trânsito CSR ou não pode encaminhar pacotes.



13. Conecte-se ao seu CSR1000v. **Note:** O nome de usuário fornecido pelo AWS para SSH no CSR1000v pode estar listado incorretamente como raiz. Altere para ec2-user se necessário. **Note:** Você deve conseguir fazer ping no endereço DNS para SSH. Aqui está ec2-54-208-234-64.compute-1.amazonaws.com. Verifique se a sub-rede/eni pública do roteador está associada à tabela de rotas públicas. Vá rapidamente para a Etapa 8 sobre como associar a sub-rede à Tabela de

Rotas.

## Connect To Your Instance ✕

I would like to connect with  A standalone SSH client  
 A Java SSH Client directly from my browser (Java required)

---

**To access your instance:**

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (HA.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:  

```
chmod 400 HA.pem
```
4. Connect to your instance using its Public DNS:  

```
ec2-54-208-234-64.compute-1.amazonaws.com
```

**Example:**

```
ssh -i "HA.pem" root@ec2-54-208-234-64.compute-1.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

[Close](#)

## Etapa 6. Repita a Etapa 5 e crie a segunda instância do CSR1000v para HA.

Sub-rede pública: 10.16.1.0/24

Sub-rede privada: 10.16.5.0/24

Se você não conseguir fazer ping do endereço IP elástico dessa nova AMI, vá rapidamente para a etapa 8 e verifique se a sub-rede pública está associada à tabela de rota pública.

## Etapa 7. Repita a Etapa 5 e crie uma VM (Linux/Windows) no AMI Marketplace.

Para este exemplo, use o Ubuntu Server 14.04 LTS no mercado.

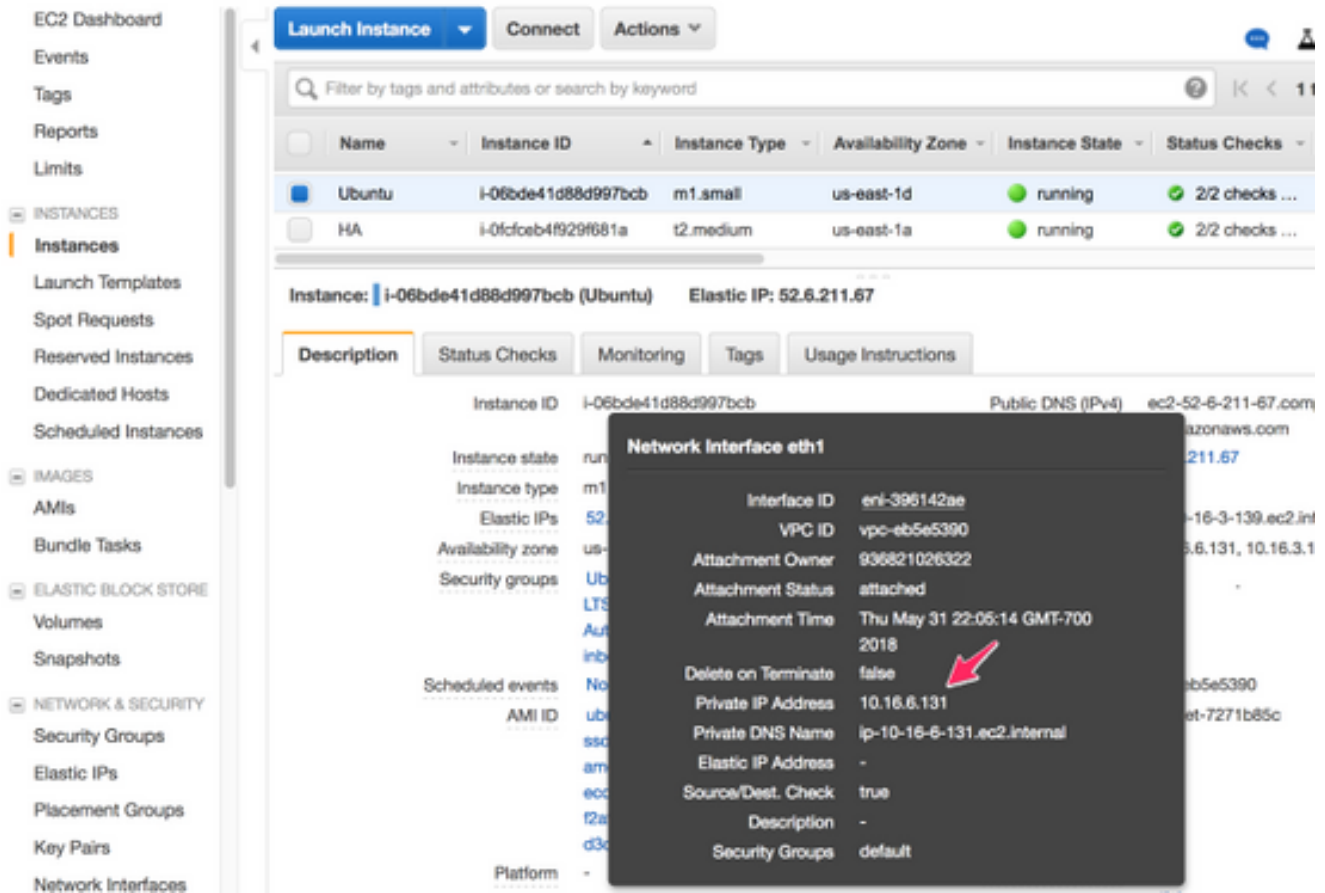
Sub-rede pública: 10.16.2.0/24

Sub-rede privada: 10.16.6.0/24

Se você não conseguir fazer ping do endereço IP elástico dessa nova AMI, vá rapidamente

para a etapa 8 e verifique se a sub-rede pública está associada à tabela de rota pública.

1. Eth0 é criado por padrão para a interface pública. Crie uma segunda interface chamada eth1 para a sub-rede privada.



2. O endereço IP configurado no Ubuntu é a interface privada eth1 atribuída pelo AWS.

```
ubuntu@ip-10-16-2-139:~$ cd /etc/network/interfaces.d/
```

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo vi eth1.cfg
```

```
auto eth1
iface eth1 inet static
    address 10.16.6.131
    netmask 255.255.255.0
    network 10.16.6.0
    up route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

3. Altere a interface ou reinicialize a VM.

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo ifdown eth1 && sudo ifup eth1
```

```
ubuntu@ip-10-16-2-139:/etc/network/interfaces.d$ sudo reboot
```

4. Faça ping para 8.8.8.8 para o teste. Certifique-se de que a rota 8.8.8.8 tenha sido adicionada de acordo com a etapa 7.

```
ubuntu@ip-10-16-2-139:~$ route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.16.2.1 0.0.0.0 UG 0 0 0 eth0
8.8.8.8 10.16.6.1 255.255.255.255 UGH 0 0 0 eth1 <-----
10.16.3.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
10.16.6.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1
```

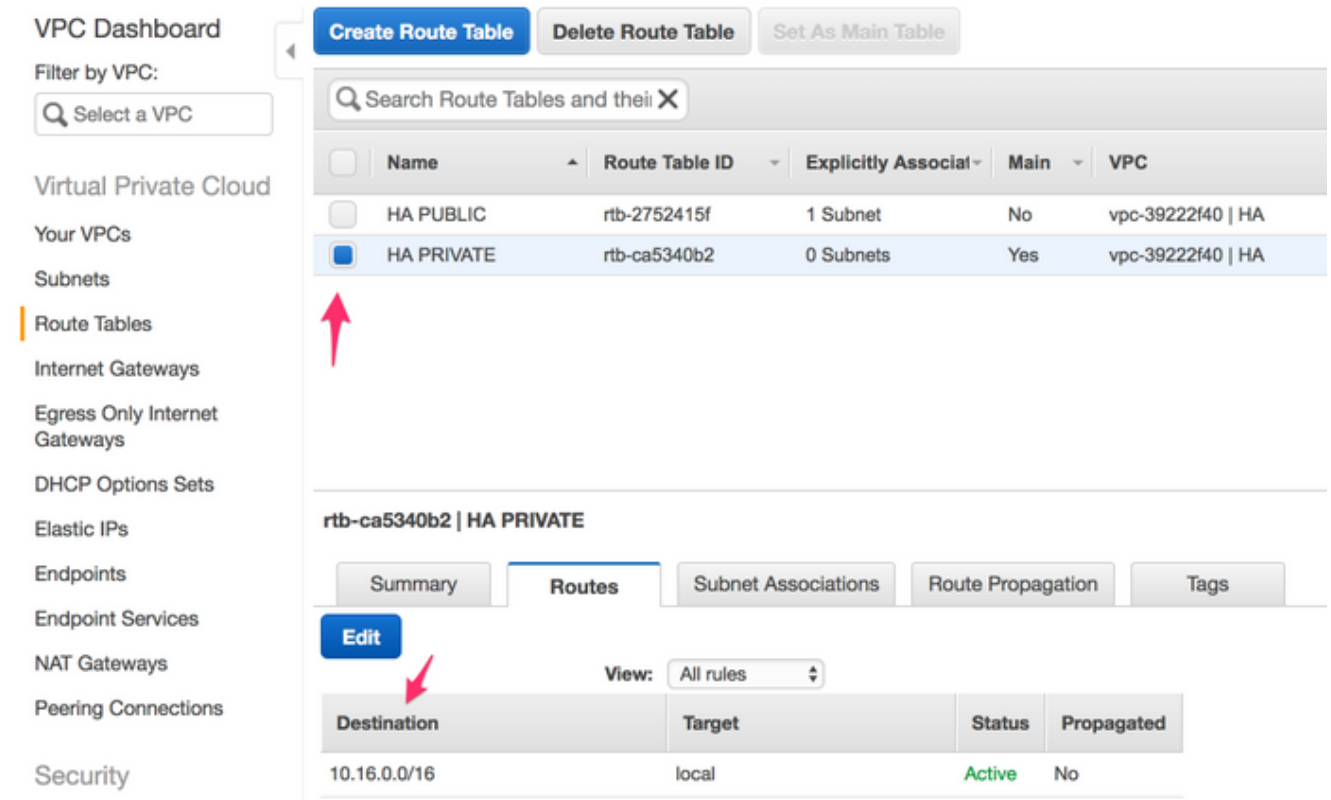
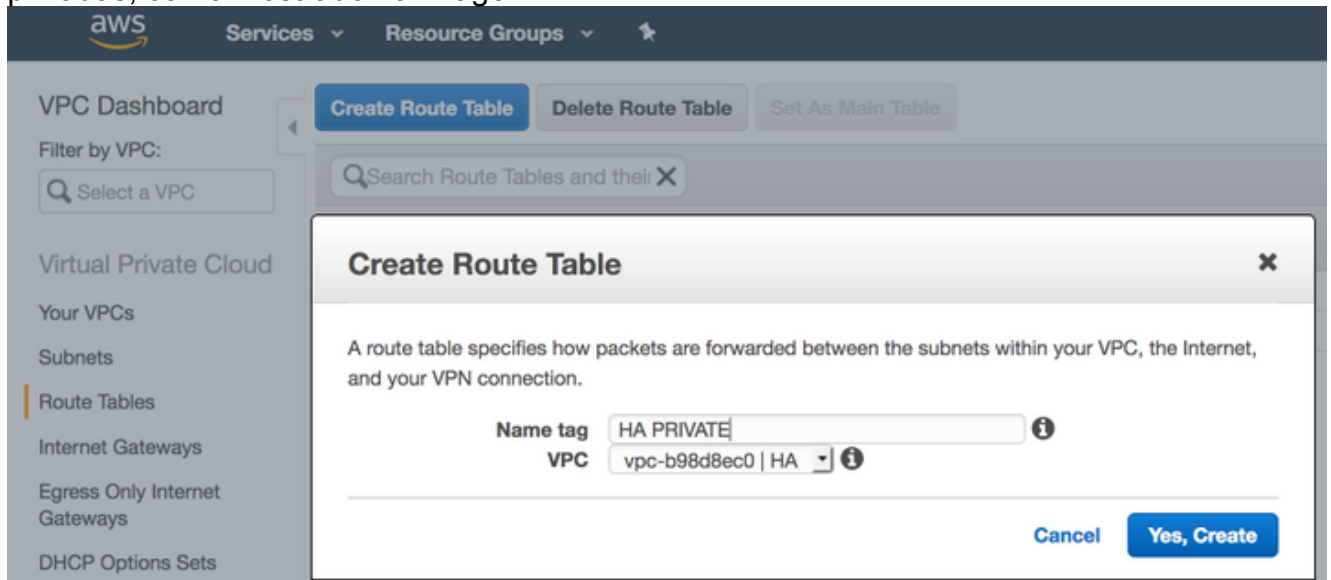
Se 8.8.8.8 não estiver listado na tabela, adicione-o manualmente:

```
ubuntu@ip-10-16-2-139:~$ sudo route add -host 8.8.8.8 gw 10.16.6.1 dev eth1
```

## Etapa 8. Configurar as tabelas de rotas privadas e públicas.



1. Quando um VPC através do assistente na Etapa 2 é criado, duas tabelas de rota são criadas automaticamente. Se houver apenas uma tabela de rota, crie outra para suas sub-redes privadas, como mostrado na imagem.



2. Esta é uma visualização das duas tabelas de rotas. A tabela de rota PÚBLICA tem o gateway de Internet (igw-95377973) anexado automaticamente. Rotule essas duas tabelas adequadamente. A tabela PRIVATE NÃO deve ter essa rota.

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables**
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

Network ACLs

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID	Explicitly Associated	Main	VPC
<input checked="" type="checkbox"/>	HA PUBLIC	rtb-2752415f	1 Subnet	No	vpc-39222f40   HA
<input type="checkbox"/>	HA PRIVATE	rtb-ca5340b2	0 Subnets	Yes	vpc-39222f40   HA

rtb-2752415f | HA PUBLIC

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No
0.0.0.0/0	igw-953779f3	Active	No

3. Associe todas as 6 sub-redes à Tabela de Rotas apropriada 3 As interfaces públicas estão associadas à tabela de rotas públicas: Sub-redes públicas: 10.16.0.0/24, 10.16.1.0/24, 10.16.2.0/24 3 As interfaces privadas estão associadas à tabela de rotas privadas: Sub-redes Privadas: 10.16.4.0/24, 10.16.5.0/24, 10.16.6.0/24

rtb-ec081d94 | HA PRIVATE

Summary Routes **Subnet Associations** Route Propagation Tags

Edit

Subnet	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations. The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:		

### Etapa 9. Configurar a conversão de endereço de rede (NAT) e o túnel GRE com BFD e qualquer protocolo de roteamento.

Configure o túnel do Generic Routing Encapsulation (GRE) através dos Elastic IPs do CSR 1000v (recomendado para evitar problemas de renovação de aluguel do DHCP, que detectam falhas falsas). Os valores BFD (Bidirection Forwarding Detection) podem ser configurados para serem mais agressivos do que os mostrados neste exemplo, se uma convergência mais rápida for necessária. No entanto, isso pode levar a eventos de peer down BFD durante a conectividade intermitente. Os valores neste exemplo detectam falha de peer em 1,5 segundos. Há um atraso variável de aproximadamente alguns segundos entre o momento em que o comando AWS API é executado e quando as alterações na tabela de roteamento do VPC entram em vigor.

- Configuração no CSRHA

## GRE e BFD - Usados para observar condições para failover de HA

```
interface Tunnell
  ip address 192.168.1.1 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 52.10.183.185 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnell
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

## NAT e roteamento - Usados para acessibilidade da Internet da VM por meio da interface privada

```
interface GigabitEthernet1
  ip address dhcp
  ip nat outside
  no shutdown
!
interface GigabitEthernet2
  ip address dhcp
  ip nat inside
  no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.4.1
```

- Configuração no CSRHA1

## GRE e BFD - Usados para observar condições para failover de HA

```
interface Tunnell
  ip address 192.168.1.2 255.255.255.0
  bfd interval 500 min_rx 500 multiplier 3
  tunnel source GigabitEthernet1
  tunnel destination 50.112.227.77 /* Elastic IP of the peer CSR */
!
router eigrp 1
  bfd interface Tunnell
  network 192.168.1.0
  passive-interface GigabitEthernet1
```

## NAT e roteamento - Usados para acessibilidade da Internet da VM por meio da interface privada

```
interface GigabitEthernet1
  ip address dhcp
  ip nat outside
  no shutdown
!
interface GigabitEthernet2
```

```

ip address dhcp
ip nat inside
no shutdown
!
ip nat inside source list 10 interface GigabitEthernet1 overload
!
access-list 10 permit 10.16.6.0 0.0.0.255
!
ip route 10.16.6.0 255.255.255.0 GigabitEthernet2 10.16.5.1

```

## Etapa 10. Configurar a alta disponibilidade (Cisco IOS XE Denali 16.3.1a ou posterior).

Monitore os eventos de peer down de BFD configurando cada CSR 1000v usando o comando cloud provider aws especificado abaixo. Use este comando para definir as alterações de roteamento para (VPC) Route-table-id, Network-interface-id e CIDR depois que um erro AWS HA, como peer down BFD, for detectado.

```

CSR(config)# redundancy
CSR(config-red)# cloud provider [aws | azure] node-id
# bfd peer ipaddr
# route-table table-name
# cidr ip ipaddr/prefix
# eni elastic-network-intf-name
# region region-name

```

1. O `#bfd peer ipaddr` é o endereço IP do túnel par.

```
CSRHA#show bfd neighbors
```

```

IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.1.2 4097/4097 Up Up Tu1

```

2. O nome de tabela `#route-table` é encontrado no console AWS, navegue para **VPC > Route Tables**. Essa ação altera a tabela de rotas privadas.

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Create Route Table Delete Route Table

Search Route Tables and their

<input type="checkbox"/>	Name	Route Table ID
<input type="checkbox"/>		rtb-7b746303
<input type="checkbox"/>	HA PUBLIC	rtb-ab091cd3
<input type="checkbox"/>		rtb-a4495edc
<input checked="" type="checkbox"/>	HA PRIVATE	rtb-ec081d94

3. O `#cidr ip ipaddr/prefix` é o endereço de destino para a rota a ser atualizada na tabela de rota. No console AWS, navegue para **VPC > Route Tables**. Role para baixo, clique em **Edit** e depois em **Add another route**. Adicione nosso endereço de destino de teste 8.8.8.8 e ENI privado de CSRHA.

rtb-ec081d94 | HA PRIVATE

Summary Routes Subnet Associations Route Propagation Tags

Edit

rtb-ec081d94 | HA PRIVATE

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
10.16.0.0/16	local	Active	No	
8.8.8.8/32	eni-10e3a018	Active	No	✕

Add another route

4. O #eni elastic-network-intf-name é encontrado na instância EC2. Clique na sua interface privada eth1 para cada um dos CSRs correspondentes e use o ID da interface.

Instances

Instance	AMI	Instance ID	Instance Type	Availability Zone	State	Health	Checks
CSRHA	i-0223f5ca1d6068424	i-0223f5ca1d6068424	c4.large	us-west-2a	running	OK	2/2 checks ...
CSRHA1	i-0bed9ff2bd6996ca4	i-0bed9ff2bd6996ca4	t2.medium	us-west-2b	running	OK	2/2 checks ...
WINDOWS	i-07a0fecde36302c6a	i-07a0fecde36302c6a	t2.small	us-west-2c	running	OK	2/2 checks ...

Instance: i-0223f5ca1d6068424 (CSRHA) Elastic Network Interfaces

Interface ID	VPC ID	Attachment Owner	Attachment Status	Attachment Time	Delete on Terminate	Private IP Address	Private DNS Name	Elastic IP Address	Source/Dest. Check	Description	Security Groups
eni-90b500a8	vpc-19c1c060	936821026322	attached	Thu May 31 21:57:41 GMT-700 2018	true	10.16.4.198	ip-10-16-4-198.us-west-2.compute.internal	-	false	-	HAKAUL

Network interfaces eth0 eth1

5. O nome do #region é o nome do código encontrado no documento AWS. Essa lista pode ser alterada ou ampliada. Para encontrar as últimas atualizações, visite o documento [Região e Zonas de Disponibilidade da Amazon](#).

Code	Name
us-east-1	US East (N. Virginia)
us-east-2	US East (Ohio)
us-west-1	US West (N. California)
us-west-2	US West (Oregon)
ca-central-1	Canada (Central)
eu-central-1	EU (Frankfurt)
eu-west-1	EU (Ireland)
eu-west-2	EU (London)
eu-west-3	EU (Paris)
ap-northeast-1	Asia Pacific (Tokyo)
ap-northeast-2	Asia Pacific (Seoul)
ap-northeast-3	Asia Pacific (Osaka-Local)
ap-southeast-1	Asia Pacific (Singapore)
ap-southeast-2	Asia Pacific (Sydney)
ap-south-1	Asia Pacific (Mumbai)
sa-east-1	South America (São Paulo)

### Exemplo de configuração de redundância no CSRHA

```

redundancy
cloud provider aws 1
  bfd peer 192.168.1.2
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-90b500a8
  region us-west-2

```

### Exemplo de configuração de redundância no CSRHA1

```

redundancy
cloud provider aws 1
  bfd peer 192.168.1.1
  route-table rtb-ec081d94
  cidr ip 8.8.8.8/32
  eni eni-10e3a018
  region us-west-2

```

# Verifique a alta disponibilidade

## 1. Verifique as configurações de BFD e nuvem.

```
CSRHA#show bfd nei
```

```
IPv4 Sessions
NeighAddr LD/RD RH/RS State Int
192.168.1.2 4097/4097 Up Up Tu1
```

```
CSRHA#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.2 Tu1 12 00:11:57 1 1470 0 2
```

```
CSRHA#show redundancy cloud provider aws 1
```

```
Cloud HA: work_in_progress=FALSE
Provider : AWS node 1
State : idle
BFD peer      = 192.168.1.2
BFD intf      = Tunnel1
route-table   = rtb-ec081d94
cidr          = 8.8.8.8/32
eni           = eni-90b500a8
region        = us-west-2
```

## 2. Execute um ping contínuo da VM para o destino. Certifique-se de que o ping esteja usando a interface eth1 privada.

```
ubuntu@ip-10-16-3-139:~$ ping -I eth1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.16.6.131 eth1: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=50 time=1.60 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=50 time=1.62 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=50 time=1.57 ms
```

## 3. Verifique a tabela de rotas privadas. O eni é atualmente a interface privada do CSRHA onde esse é o tráfego.

rtb-ec081d94 | HA PRIVATE

Summary	Routes	Subnet Associations	Route Propagation	Tags
<a href="#">Edit</a>				
View: <input type="text" value="All rules"/>				
Destination	Target	Status	Propagated	
10.16.0.0/16	local	Active	No	
8.8.8.8/32	eni-90b500a8 / i-0fcfceb4f929f681a	Active	No	

## 4. Desligue o Tunnel1 do CSRHA para simular um failover de HA.

```
CSRHA(config)#int Tu1
CSRHA(config-if)#shut
```

## 5. Observe que a tabela de rotas aponta para o novo ENI, que é a interface privada do CSRHA1.

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit

View: All rules ▾

Destination	Target	Status	Propagated
10.16.0.0/16	local	Active	No
8.8.8.8/32	eni-10e3a018 / i-0fcfceb4f929f681a	Active	No

## Troubleshoot

- Verifique se os recursos estão associados. Ao criar VPC, Sub-redes, Interfaces, Tabelas de Rotas etc., muitos deles não são associados entre si automaticamente. Eles não têm conhecimento um do outro.
- Certifique-se de que o IP elástico e qualquer IP privado estejam associados às interfaces corretas, com as sub-redes corretas, adicionadas à tabela de rotas correta, conectadas ao roteador correto e ao VPC e zona corretos, vinculados à função IAM e aos grupos de segurança.
- Desabilitar verificação de Origem/Destino por ENI.
- Para o Cisco IOS XE 16.3.1a ou posterior, estes são os comandos de verificação adicionais disponíveis.

```
show redundancy cloud provider [aws | azure] node-id
debug redundancy cloud [all | trace | detail | error]
debug ip http all
```

- Aqui estão as falhas comuns observadas nas depurações:

### Problema: falha na httpc\_send\_request

Resolução: O HTTP é usado para enviar a chamada à API do CSR para o AWS. Verifique se o DNS pode resolver o nome DNS listado na sua instância. Verifique se o tráfego http não está bloqueado.

```
*May 30 20:08:06.922: %VXE_CLOUD_HA-3-FAILED: VXE Cloud HA BFD state transitioned, AWS node 1
event httpc_send_request failed
*May 30 20:08:06.922: CLOUD-HA : AWS node 1 httpc_send_request failed (0x12)
URL=http://ec2.us-east-2b.amazonaws.com
```

### Problema: a tabela de rota rtb-9c000f4 e a interface eni-32791318 pertencem a redes diferentes



**Resolução:** O nome da região e o ENI estão configurados incorretamente em redes diferentes. A região e o ENI devem estar na mesma zona que o roteador.

```
*May 30 23:38:09.141: CLOUD-HA : res content iov_len=284 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>InvalidParameterValue</Code><Message>route table rtb-9c0000f4 and
interface eni-32791318 belong to different
networks</Message></Error></Errors><RequestID>af3f228c-d5d8-4b23-b22c-
f6ad999e70bd</RequestID></Response>
```

**Problema: Você não está autorizado a executar esta operação. Mensagem de falha de autorização codificada.**

**Resolução:** Função/política IAM JSON criada incorretamente ou não aplicada ao CSR. A função IAM autoriza o CSR a fazer chamadas de API.

```
*May 30 22:22:46.437: CLOUD-HA : res content iov_len=895 iov_base=<?xml version="1.0"
encoding="UTF-8"?>
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not authorized to
perform this operation. Encoded
authorization failure message: qYvEB4MUdOB8m2itSteRgnOuslAaxhAbDph5qGRJkjjJbrESajbmF5HWUR-
MmHYeRALpKZ3Jg_y-
_tMlYe15l_ws8Jd9q2W8YDXBl3uXQqfW_cjJrgy9jhnGY0nOaNU65aLpfqui8kS_4RPOpm5grRFFfo99-
8uv_N3mYaBqKFPn3vUcSYKBmxFIikJKcJy9esOeLlOWDcnYGGu6AGGMoMxWdtk0K8nwk4IjLdCnd2cDXeENS45w1PqzKGPsh
v3wD28TS5xRjIrPXyrT18UpV6lLA_09Oh4737VncQKfzbz4tPpnAkoW0mJLQ1vDpPmNvHUpEng8KrGWYNfbfemoDtWqIdABf
aLLm4saNtnQ_OMBOTi4toBLEb2BNdMkl1UVBIxqTqdFUVRs**MSG 00041 TRUNCATED** **MSG 00041
CONTINUATION
#01**qLosAb5Yx0DrOsLSQwzS95VGvQM_n87LBHYbAWWhqWj3UfP_zmiak7d1m9P41mFCucEB3Cs4FRsFtb-
9q44VtyQJaS2sU2nhGe3x4uGEsl7F1pNv5vhVeYOZB3tbOfbV1_Y4trZwYPPfGLKgBShZp-WNmUKUJJsKcl-
6KGqmp7519imvh66Jgwgmu9DT_qAZ-jEjkqWjBrxg6krw</Message></Error></Errors><RequestID>4cf31249-
2a6e-4414-ae8d-6fb825b0f398</RequestID></Response>
```

## Informações Relacionadas

- [Redundância de gateway VPC - Cisco](#)
- [Guia de implantação do roteador de serviços em nuvem Cisco CSR 1000v Series para serviços da Web da Amazon](#)
- [Divisão de tipos de instância](#)
- [EC2 e VPCs](#)
- [Interfaces de rede elásticas, do Guia do usuário EC2, inclui o número de ENIs por tipo de instância](#)
- [Como fazer - Redes aprimoradas no Linux, informações de apoio úteis](#)
- [Instâncias dedicadas/explicações de locatário e como fazer](#)
- [Documentação geral do EC2](#)
- [Documentação geral do VPC](#)
- [Regiões e Zonas de Disponibilidade](#)
- [CSR1000v High Availability versão 3](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.